Group Homework – Questions and Answers from Readings

Michael Aguilar, Wade Astin, Jacob Frimpong and Kevin Scharnhorst

MED INF 403 – Introduction to Medical Informatics, Spring 2010

Northwestern University

From Biomedical Informatics text, chapters 7 and 10:

1) How have some of the standards discussed in the chapter impacted policies and procedures on the job for you or others you work with?

Working as a software developer in the insurance industry I have seen how standards discussed in the chapter reading impacts my organization. The effects can be perceived both good and bad. On the negative side standards can sometimes be perceived as controlling. They add more work to an already busy organization. Implementation generally requires modification to existing processes in order to comply. In cases where compliance is mandated, the work involved and aggressive timeline can add stress to an organization to implement correctly and on time. In addition implementations are generally audited. Organizations such as health plans go under regular audits to ensure ongoing compliance. So standards and compliance to them can also carry monetary consequences if an organization is found non-compliant. So it becomes beneficial to the organization to invest needed financial funds to stay within check. So from this perspective, the added work, stress and cost to implement can be taken as negative.

Conversely, standards offer guidance and needed structure. Compliance offers benefits of uniformity so that organizations can interchange data between each other. An example from a payer's perspective is with the Uniform Billing Form of 1992 (UB-92). This standard serves as an example implemented through the Ad hoc method. The National Uniform Billing Committee (NUBC) was brought together by the American Hospital Association (AHA) in 1975 and it includes the participation of all the major national provider and payer organizations. It was formed to develop a single billing form and standard data set that could be used nationwide by institutional providers and payers for handling health care claims. (http://www.nubc.org/history.html). UB-92 was a result of this committee. The form benefits providers and payers and establishes a means for billings to be submitted and paid based on an industry standard. For an example of a form, see here (http://www.jrsa.org/dvsa-drc/minnesota/MN_mdh_hospital.pdf)

2) What is ANSI, IEEE, HL7, and WHO? What are their various roles in creating standards?

- ANSI – founded in 1918. Responsible for approving official *American National Standards*. ANSI membership includes over 1,100 companies; 30 government agencies and 250 professional, technical , trade, labor and consumer organizations. They do not write standards, rather they assist in the development and facilitate developers and governments recognize the need for standards. *Biomedical informatics: Computer Applications in Health Care and Biomedicine. pp 272*.
- IEEE – An international organization that is a member of both ANSI and ISO. Standards in telecommunications, electronics, electrical applications, and computer related standards have all been products of the IEEE organization. *Biomedical informatics: Computer Applications in Health Care and Biomedicine. pp 302.*

- HL7 – founded in 1987. The group adopted the name HL7 to reflect the application (seventh) level of the OSI reference model. The primary goal of the organization was to provide a standard interchange exchange for transmitting data among hospital computer applications. It supports exchanges single and batch transmissions. HL7 has over 500 organizational members, and over 2,200 individual members. It is the most widely implemented health care data-messaging standard and is in use at over 1,500 care facilities. Its reach in implementation is global. *Biomedical informatics: Computer Applications in Health Care and Biomedicine. pp 301.*
- WHO – World Health Organization. Responsible for providing leadership on global health research agenda, setting norms and standards, articulating evidence-based policy options, providing technical support to countries and monitoring assessing health trends. (http://www.who.int/about/en/). Credited in the text as having republishing ICD terminologies as recent as 1992. *Biomedical informatics: Computer Applications in Health Care and Biomedicine. pp 281.*

The various roles in creating standards include;

- *Ad hoc method*: This involves general consensus among a group of interested people or organizations. The specifications are informal in nature. Examples given in the text include laboratory system and hospital-system vendors. The American College of Radiology and DICOM standard for medical imaging are a couple examples specifically given as examples from the text.
- *De facto method*: When a single vendor by virtue of their market share establishes a standard and it is accepted by the industry due to the market influence of that vendor. Microsoft Windows is an example from the text. Another example might include Adobe Portable Document Format (PDF).
- *Government –mandate method*: A government agency creates a standard and legislates implementation of in an industry. The text's exmpale is CMS's UB92 insurance claim form.
- *Consensus method*: Driven by volunteers representing interested parties. Most standards are created by this method. The text uses Health Level 7 (HL7) as an example.

Biomedical informatics: Computer Applications in Health Care and Biomedicine. pp 269.

3) Give an example of when social, legal or personal ethics might come into conflict in the practice of medicine. Consider and write about the different perspectives of three of the following: physicians, nurses, patients, pharmaceutical professionals, ancillary healthcare providers, and hospitals. You may also choose to write about a healthcare professional not listed.

Providers of medicals services are aware that that they have a moral and legal obligation to protect patient medical information but cost and resources many hinder them from implementing security procedures. In order to protect patient information providers need to add modules to their health information systems that prevent unauthorized or unnecessary access to patient information. Health information systems can be financially expensive to change especially for smaller organizations that do not have large IT budgets. Many providers may thus he hesitant to make the needed IT

upgrades. Patient data security policies and procedures must be developed to protect patient data and a staff must be place to make sure those policies and procedures are implemented. Employees must also be trained on the issue of protecting patient data. The staff resources to implement policies and monitor the system may not be available at some provider organizations. Providers may thus chose not to spend the resources to make sure the system is actually working.

Physicians

The administration staff of the outpatient physician office must be adequately trained on HIPPA and patient health information security. The staff have access to patient medical records and patient medical claims. Thus there is the potential for unauthorized or unnecessary access to patient medical information. Most physicians are too busy to monitor their staff to see if they are following HIPPA regulations or internal patient security procedures. Physician need to assign staff to monitor and implement the patient information policies and procedures. Physicians also need to make sure policies are place to hire trustworthy staff.

Ancillary healthcare providers

Ancillary health providers often need to exchange result data with physician groups and health plans. The exchange data system must be secure and the system must encrypt the patient data before it is sent out. The staff needed to monitor this system must be adequately trained to monitor and maintain the system. Ancillary healthcare providers may be hesitant due to high training costs to adequately train their personnel. The management of ancillary providers must show leadership in this area and provide their IT departments will adequate training resources.

Hospitals

In hospitals different departments like pharmacy, nursing, and imaging can have access to a patient's medical record. If the hospital has an EMR system then potentially additional personal will have access to the record. Hospitals need staff and policies in place to protect against unauthorized access to patient health information. In order to save money hospitals may create policies but not allocate adequate resources to monitor and implement the system. The hospital board must show leadership and adequately fund the patient data security department.

Article #1 - Informed Consent to the Secondary Use of EHRs(Kluge):

1) Describe how general principles of ethics are applied to confidentiality issues surrounding the EMR

Prevailing opinion is that secondary use of data requires informed consent based on 3 concepts….

1. Patients have privacy rights
2. Privacy arrangement between patient and provider
3. Patient has a proprietary interest in their data as the primary source

However, these concepts do not prove that it is unethical to access nor that consent is always required…for example, these are given as examples when consent is not needed…

1. Access to data Integral to patient care
2. Restricted access can jeopardize rights of third parties
3. Data is needed for bona-fide research
4. Necessary for development of maintenance of system

General ethics principles are below in the context of informatics …

1. Autonomy>right of privacy> integrity of the person**:** Autonomy is essentially the right to self determination, but not to the extent of interfering with equal and competing rights of others….therefore, withholding some data could harm others.
2. Equality
3. Duty to prevent harm (malfeasance)
4. Impossibility--person cannot be held to what is impossible. Example: patient enters a system with the expectation of care, and that care produces data, and it is impossible to withhold that from users who have a legitimate access to that record.
5. Duty to advance good of others (beneficence)…if information collected will advance a cause, then sharing of that data is ethically grounded.

Limitations of principles: allows for some breach of confidentiality; however limitations must exist to prevent voyeurism and trespassing. Ideally, consent obtained at the time record is established. Limitations are…

1. Data release may not go beyond what is demonstrably necessary.
2. Least intrusive amount of information.
3. Minimum of interference to person.
4. De-identifiy data if possible.
5. Tight audit trails are needed.

Possible EMR policy models to follow…

1. *Automatic authorized access model*. Access to all who are actively engaged in care on need to know basis without consent; Appropriate security measures in place; Patients would be notified of breaches; Must allow patient to restrict but only with explanation that they might jeopardize optimal care .
2. *Modified access model*: some data is stripped of identifying information and then shared with authorized; Tracking and surveillance still required.
3. *Explicit consent Model*: Patients would be asked EACH TIME that the data about them is generated. Again, would need to accompany understanding that withholding information may jeopardize patients care.

4. *Two-stage model* (combo of other models)…access to identified data is available upon explicit consent; de-identified data can be shared.

In short, not all secondary and non consensual uses of the HER are inherently unethical

Article #2 : ***Privacy-Preserving Data Releases for Health Report Generation:***

1) What are the challenges of publishing data and yet retaining privacy?

Publishing data can potentially allow the inferential disclosure of private and confidential information. Even where statistical properties of data are published instead of specific single tests, the data may be subject to interval inference (through the application of Non-Linear Programming) if not handled properly. Inferential disclosure can allow:

a. The disclosure of patient information,
b. The provider's data to be inferred by competitors,
c. Unsecured data infrastructure of the mediator/provider to be accessed by external hackers,
d. Malicious/disgruntled employees of provider to cause harm, and
e. Incompetent staff on provider's side to unintentionally grant data access to unauthorized parties

It should be noted that the HIPAA Privacy Rule establishes minimum Federal standards for protecting the privacy of individually identifiable health information and establish conditions under which covered entities (health plans, health clearinghouses, or a health care provider who transmits information in electronic form) can provide researchers access to and use of Protected Health Information (PHI) when necessary to conduct research.

2) What are some of the remedies proposed by the authors (Padman) to provide access without breaching confidentiality?

a. The provider should conduct an internal disclosure audit or disclosure detection on the data before their data can be given to the mediator. Audit and aggregate methodology to detect and limit interval inference. The provider can specify the maximum disclosure risk for each of their sensitive cells. If a disclosure is detected, then the data publication that was proposed by the mediator cannot take place.

b. The provider can limit disclosure by systematic aggregation and by making the marginal information fuzzier without compromising the data's usefulness for the legitimate user.

c. Encryption of data

d. De-identification or Anonymization (using statistical verification or by removing certain pieces of information from each record as specified in the HIPAA Privacy rule).

e. Certify mediator as trusted third party that does not store data persistently and only uses it for report generation